Sandstorm Enterprises

Sandtrap 1.5
User Manual

[This Page Intentionally Blank]

Table of Contents

Legal Notices

Sandtrap may only be used by authorized licensees, who agreed upon installation to all of the terms and conditions of the end user license below:

End User License Agreement

Sandstorm Enterprises Inc. ("Sandstorm") and/or its suppliers own these programs and their documentation, which are protected under applicable copyright laws. Your right to use the programs and the documentation is limited to the terms and conditions described below.

1. License:

YOU MAY: (a) use the enclosed programs on a single computer; (b) physically transfer the programs from one computer to another provided that the programs are used on only one computer at a time, and that you remove any copies of the programs from the computer from which the programs are being transferred; (c) make a copy of the programs solely for purposes of backup. The copyright notice must be reproduced and included on a label on any backup copy.

Sandstorm reserves all other rights, including, but not limited to, the following:

YOU MAY NOT: (a) distribute copies of these programs or their documentation to others; (b) rent, lease or grant your rights to others; (c) alter the programs or their documentation without the prior written consent of Sandstorm; (d) disassemble or reverse engineer the programs; or (e) ship or transmit (directly or indirectly) any copies of the programs or its media, or any direct product thereof, to any country or destination prohibited by the United States Government.

2. Term:

Your License remains effective until terminated. You may terminate it at any time by destroying the distribution media together with all copies of the programs in any form, and returning the hardware license management device ("dongle") to Sandstorm or destroying it if returning it is not possible. Your License will also automatically terminate without notice if you fail to comply with any term or condition of this Agreement. Upon termination you must destroy all copies of the programs in any form.

3. Limited Warranty, Disclaimer and Limitation of Liability:

Sandstorm and Vendor warrant the media on which the Licensed Programs are provided to be free from defects in materials and workmanship for 90 days after delivery. Defective media may be returned for replacement without charge during the 90-day warranty period unless the media has been damaged by accident or misuse. Due to the complex nature of computer software, Sandstorm does not warrant that the Licensed Programs are completely error-free, will operate without interruption, or are compatible with all equipment and software configurations. DO NOT USE THE LICENSED PROGRAMS IN ANY CASE WHERE SIGNIFICANT DAMAGE OR INJURY TO PERSON, PROPERTY OR BUSINESS MAY HAPPEN IF ANY ERROR OCCURS. YOU EXPRESSLY ASSUME ALL RISK FOR SUCH USE, AND FOR ANY VIOLATION OF STATE OR FEDERAL LAW THAT MAY RESULT.

Repair, replacement or refund (at the option of Sandstorm) is the exclusive remedy if there is a defect. SANDSTORM MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, WITH RESPECT TO THE LICENSED PROGRAMS, THEIR MERCHANTABILITY, OR THEIR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL SANDSTORM BE LIABLE FOR INDIRECT OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATIONS, LOSS OF INCOME, USE OR INFORMATION, NOR SHALL THE LIABILITY OF SANDSTORM EXCEED THE AMOUNT

PAID FOR THE LICENSED PROGRAMS. THE LICENSED PROGRAMS ARE NOT INTENDED FOR PERSONAL, FAMILY OR HOUSEHOLD USE.

Any suit or other legal action relating in any way to this Agreement or to the Licensed Programs must be officially filed or officially commenced no later than one (1) year after it accrues. This warranty gives the customer specific legal rights, and you may also have other rights which vary from state to state.

4. General terms:

The License shall not be assigned or transferred without the written consent of Sandstorm. The validity, construction and performance of this Agreement is governed by the laws of the Commonwealth of Massachusetts, without regard to Massachusetts choice-of-law rules. Suit or arbitration relating to this Agreement may be brought only in Massachusetts.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT IT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN YOU AND SANDSTORM, AND SUPERSEDES ANY EARLIER PROPOSAL OR PRIOR ARRANGEMENT, WHETHER ORAL OR WRITTEN, AND ANY OTHER COMMUNICATIONS BETWEEN YOU AND SANDSTORM RELATING TO THE SUBJECT OF THIS AGREEMENT.

1 Introduction

Welcome to Sandtrap!

Sandtrap™ is a telephone system intrusion detection tool that can detect attempts to access your organization's computer systems through the telephone network. Sandtrap is designed to detect and identify attackers who are engaged in telephone scanning, also known as "war dialing." Sandtrap can also be used to audit the activities of commercial telephone scanners such as Sandstorm's PhoneSweep. Sandtrap is an important threat assessment tool that can alert you if and when your organization is under attack. In many cases, Sandtrap can even help you identify the perpetrators.

1.1 Why Worry About Unauthorized Telephone Scans?

Despite the attention given to Internet connections and firewalls, hostile telephone scanning (a.k.a. "war dialing") remains one of the most powerful means for computer attackers to assess and penetrate a target organization.

Most organizations locate all of their telephone extensions within a block of telephone numbers that are rented from a telephone company. By dialing every telephone number in an organization's block, an attacker can locate unsecured or misconfigured modems that allow access to computer systems and networks. There are many documented cases in which a single misconfigured computer modem has compromised the security of an entire organization.

Equipped with additional information, such as an employee list, a list of accounts, or valid username/password combinations, an attacker is even more likely to penetrate a computer system's misconfigured dial-up modem.

Several companies sell "telephone firewalls" that can intercept and terminate inbound data calls to phone numbers that are not authorized to host inbound modems. However, these systems can be very expensive and constitute a single point of failure for an organization's entire telephone system.

1.2 Sandtrap: A Telephone Threat Assessment Tool

Sandtrap is a program that will alert you when someone attempts to penetrate your computer systems through telephone scanning.

Sandtrap runs on a computer equipped with one or more dial-up telephone lines.

- Runs on industry-standard Windows 95, 98, NT, 2000 and XP platforms.

- Watches the modems and waits for an incoming telephone call.

- Notes the Caller ID information associated with incoming calls.

- Directs the modem to answer incoming calls with a data tone.

- Prompts the caller for a username and password, then displays a message and hangs up on the caller.

- Logs the time of the call, the phone number of the caller, the username and the password that were provided.

- Sends the log information to you by email or through a web-based alert.

- Comes in versions that can monitor one, four, eight, twelve, or sixteen modems.

Sandtrap cannot stop somebody from telephone scanning your organization, but it can tell you if you are under attack. If your organization is being actively scanned, you may wish to perform your own telephone scan, so that you may detect and disable any vulnerable modems before the outside attacker can use them. Since most attackers use a single phone line, with a multi-line version of Sandtrap you will be able to detect multiple attacks simultaneously, or detect in one session the same attacker calling multiple lines.

Sandtrap may also provide you with the information necessary to make the telephone scanning stop. Many attackers unwittingly place telephone calls from their home phones without first blocking Caller ID. By capturing Caller ID information, Sandtrap may provide you with the name and phone number of your attacker. Even if Caller ID information is not available, by capturing the usernames that the attacker provides, you may be able to infer whether the attacker is an insider or an outsider. Finally, the Sandtrap log files and alert messages can be used as evidence in a court of law.

Sandtrap was designed and written specifically as a security audit tool by an experienced team of engineers and security professionals. Sandtrap is designed to be easy to use, flexible, and powerful.

1.3 New Features for Sandtrap 1.5

Sandtrap 1.5 includes many new features, listed here:

- Multiple login tries.

- Configurable "bad password" prompt for between login tries.

- Option to display banner between login tries.

- "Trap" mode to keep caller on line, with configurable prompts and messages.

- Emulation and trap mode properties can be set for each modem.

- Additional alerts after answer and entering trap mode.

- New button to revert to default emulation and trap mode settings.

- Login prompt is optional, allowing emulation of password-only systems.

- Settable pause duration at end of call.

- Modems tab items are now tab stops.

2 Installation and Setup

This section guides you through the process of getting ready to run Sandtrap. To successfully install and begin using Sandtrap, you must:

- Have HTML Help installed on your computer (to view the online manual).

- Select appropriate modems for your computer.

2.1 System Requirements

2.1.1 Monitoring Computer

If Sandtrap will be in continuous operation or will be mission critical, we recommend that you install Sandtrap on a well-maintained PC with up-to-date software (e.g. relevant service packs installed and latest drivers). Also, both the PC and Sandtrap should be tested before you leave Sandtrap running for extended periods of time. This is especially true where the intended system has previously had problems with other software, or when you intend to use Sandtrap at multiple locations and conditions.

Minimum requirements: **For 1 modem (Sandtrap Basic)**: 400 MHz PC or laptop, with 32MB RAM, Intel Celeron/PII, and 20MB of free space to store the Sandtrap program and the log files it creates.

2.1.2 Operating System

Sandtrap is certified to run under Microsoft Windows 95, 98, NT 4.0, 2000, and XP. We do not recommend or support using Sandtrap on Windows ME. **If you have a choice of platforms, we recommend that you install Sandtrap on a computer using Windows 2000** or **Windows 98**, as these are the two most stable platforms we have found to date.

Note on laptop computers and Windows NT: Sandstorm has noted that our communications programs have historically had more problems running on laptops with Windows NT than on laptops running Windows 98 or 2000, especially on laptops equipped with multi-port serial cards. Sandstorm supports NT platforms, but recommends that, if possible, users who wish to run Sandtrap on a laptop computer use Windows 98 or 2000.

2.1.3 Modem and multi-port serial I/O hardware recommendations

Follow the links on our main website (http://www.sandstorm.net) for the most up-to-date information on modem and hardware recommendations. If you are using multiple modems, you may need to use a multi-port serial I/O card.

Sandtrap works with most modems and multi-port serial cards. If your modem supports Caller ID and you use Sandtrap with a Caller ID equipped phone line, Caller ID information will automatically be captured.

- Rockwell/Conexant modems that specifically mention support for "Simultaneous Voice and Data" (SVD) will almost always report Caller ID information.

- *Avoid using modems made before 1997*, as they may not properly support Caller ID.

- Many modems that do not support Sandstorm's Single Call Detect feature will nevertheless support Caller ID. You may wish to consult your modem's documentation.

Since Sandtrap communicates with the modems directly through the serial port, you do not have to install the drivers provided with the modem.

Our most recommended analog modem is the **Zoltrix External Rainbow 56K** modem, which we can provide within the U.S. and which is sold worldwide. Other modems that we recommend are the Multi-Tech MultiModem MT5600 ZDXV, and EXP Computer's ThinFax 56L (model # MF-PCA56-L), both of which are also sold worldwide. For ISDN monitoring we recommend the U.S. Robotics Courier Imodem.

For Sandtrap Plus 16, we recommend that you use the Multi-Tech MultiModem MT5600 ZDXV (see below for further details).

For Sandtrap Plus 4, the multi-port serial I/O cards we recommend most often are SeaLevel's Versa COMM +4 or +8 Serial I/O PCI cards for PCs and Quatech's QSP 100 PCMCIA cards for laptops. (Each QSP 100 card supports up to 4 modems.) We also have SeaLevel's Seaport box, which connects to a USB port and provides 4 serial ports.

Windows NT users please note: Windows NT does not support the use of multiple multi-port serial I/O cards, which limits Windows NT laptops to using only one QSP 100 PCMCIA card and desktops to using only one SeaLevel Versa COMM +8.

Windows 2000 users please note: If installing a SeaLevel card that you have owned for more than a year on Windows 2000, make sure that you have the latest drivers from SeaLevel, dated January 2001 or later. The old SeaLevel drivers (Pre-Jan. 2001) may cause your system to freeze.

For Sandtrap Plus 16 (desktops only), we recommend the use of:

- Multi-Tech ZDX Modem Rack (http://www.multitech.com) which takes up to 12 Multi-Tech MT5600ZDXV modems. (For Sandtrap Plus 16, you would need to place 4 standard Multi-tech MT5600ZDXV modems to the side).

- Digi AccelePort 16em (http://www.digi.com) multi-port, which provides 16 serial I/O ports for your desktop, connecting through a PCI card.

- Digi EdgePort, which connects to a USB port and provides 16 serial I/O ports for a laptop or a desktop.

2.1.4 Modem Phone Line(s)

Modem phone lines should be dedicated analog or ISDN phone lines. For optimal detection, you should use phone lines that are located within the block of phone numbers used most frequently by your organization, since these are more likely to be attacked.

2.1.5 Security

Although every effort has been to provide for the security of the Sandtrap product, as with any complicated piece of software there is always a chance that an attacker may find a way to compromise the integrity of the underlying system. Therefore, if your organization requires the highest level of security, Sandtrap should be run on a computer that is not connected to a network. This will mean that you will not receive email alerts. For most uses, Sandtrap can be run on a computer that is connected to both the telephone line and the computer network, provided that you have followed all standard security precautions (including installation of all patches and software updates).

2.2 Preparing to install and run Sandtrap

Before you install, reinstall, upgrade, or run Sandtrap, prepare your computer by following these steps:

- **If you are installing Sandtrap Plus 4 or 16 for the first time,** we recommend that you install multi-port cards with their respective COM ports before installing Sandtrap. Make sure that your PC can see the COM ports. This helps to separate hardware install problems from Sandtrap problems. (**Note:** SeaLevel cards require you to install the drivers before the hardware).

- **Disable your PC's power management software**. Because of bugs in some power management drivers, computers with active power management may occasionally enter "sleep" mode while Sandtrap is running, effectively turning off the hard drive and causing Sandtrap to cease execution.

- **Disable your PC's fax software**. Most fax software cannot share COM ports with Sandtrap.

- **Disable your PC's screen saver**. Some screen savers require a substantial amount of computational power in order to run. Others place the computer into "sleep" mode, even if power management is disabled. In order to minimize any possibility of conflict, we recommend that all screen savers be disabled before installing or running Sandtrap. If your screensaver does interfere with Sandtrap's operation and you need to lock or password protect your screen, we recommend using **Screen Lock**. It works on Windows 95, 98, NT 4.0, 2000, and XP, and allows you to run Sandtrap and other programs in the background. You can download it from http://www.screenlock.com.

- **Clear your PC's outgoing phone line**. Sandtrap may encounter problems sharing a local phone line with other functions. Lines with voicemail configured and/or fax machines on the same phone line as Sandtrap may respond to incoming calls, preventing Sandtrap from doing so.

- **Log in using an administrator account (Windows NT/2000/XP only)**. On Windows NT, 2000, and XP machines, Sandtrap installs a service to handle communications with the hardware license manager. If an administrator does not install Sandtrap, the installation process will fail.

- **If you are running Windows NT, 2000, or XP, attach the hardware license management device (the "dongle") to the computer's parallel or USB port**. Sandtrap will not install correctly on NT/2000/XP systems if the dongle is not attached during the installation.

2.3 Installing Sandtrap

Note that you cannot reinstall or upgrade Sandtrap while the program is running. If an attempted installation results in an error message indicating that Sandtrap is running, you can use the Task Manager (accessed by pressing CTRL-ALT-DELETE) to terminate the program. You may also reboot your computer.

Insert the Sandtrap CD-ROM into your CD-ROM drive. Sandtrap is distributed as an industry-standard InstallShield package to allow easy installation and removal. If you have not disabled Autorun, the installer will start up automatically after the drive closes. If the installer does not start automatically, select Start and then Run from the Windows startup menu, and use Browse to locate and run the program *setup.exe*. In either case, a standard InstallShield installer will guide you through the installation process. You will not need to place the Sandtrap CD-ROM in the drive to run Sandtrap after it is installed.

Sandtrap's default installation directory is: C:/Program Files/Sandstorm/Sandtrap.

If you have problems installing Sandtrap, please consult Appendix C: Sandtrap Troubleshooting Guide.

2.4 Hardware License Protection

Sandstorm Enterprises uses hardware license management devices (dongles) to prevent unauthorized use of its software. Sandtrap works with another Sandstorm product, the PhoneSweep phone line scanner, to uncover operational security information about your organization. This information could potentially be very damaging if misused. It is important that Sandtrap only be used by those authorized to do so. Therefore, to help ensure that unauthorized persons do not use Sandtrap, a **dongle is shipped with Sandtrap. This device must be attached to the computer's parallel or USB port for Sandtrap to function.** Sandtrap ships with a parallel port dongle. A USB dongle can be substituted for a small extra charge. Laptop users may wish to use the USB dongle.

Sandtrap will not run or receive calls for more than 5 minutes if the dongle is detached.

<u>**Do not remove the dongle while Sandtrap is running!**</u> Sandtrap will cease to function properly if the dongle is removed. If the dongle is disconnected while Sandtrap is running, it will be necessary to shut down Sandtrap, reattach the dongle, and restart Sandtrap.

Sandtrap's standard dongle works with most PC parallel ports, and does not preclude other simultaneous use of the parallel port. (If you have ordered Sandtrap with a USB dongle, see *Instructions for installing the optional USB dongle.*) The parallel dongle works with:

- Standard parallel ports
- Bi-directional parallel ports
- ECP ports
- EPP ports
- Most other PC parallel ports

You can attach other devices to your computer's parallel port while the dongle is in place. You can attach peripherals such as a Zip drive, a Visioneer PaperPort, another vendor's dongle, or even a printer. When attaching another device to the same parallel port as a Sandtrap dongle, connect the dongle directly to the computer and connect the other device to the dongle.

2.4.1 Laptop models known to have problems with the dongle

Sandstorm has encountered a few hardware-specific problems with the dongle.

- On most Dell laptops, the external floppy drive cannot be used through the dongle.
- The parallel port dongle does not work with Toshiba Tecra 700 series laptop computers. The problem is limited to the 700 series of Toshiba laptops; the Toshiba Portege 7020 model and other Toshiba laptops are reported to work properly**.**
- On some laptops, the parallel port may not automatically activate if the laptop is running on battery power. In this case a device with its own power supply, such as a printer or fax machine, needs to be plugged into the laptop.

If Sandtrap is unable to detect the parallel port dongle on a laptop, please contact Sandstorm; the USB dongle may suit your circumstances better.

Check Appendix C: Sandtrap Troubleshooting Guide if you have problems with the dongle. After trying the suggestions there, if you are still having problems with the dongle, contact Sandstorm Enterprises technical support at *support@sandstorm.net.*

2.4.2 Software known to interfere with dongles on the parallel port

Some printer drivers may interfere with the dongle. Other software that uses the parallel port may also interfere. A list of specific software that interferes with the dongles on parallel ports will be forthcoming on our web site.

2.4.3 Instructions for installing the optional USB dongle

Sandstorm now offers a USB dongle as an alternative to the parallel port dongle for Windows 98, 2000, and XP systems only. **The USB dongle should be installed before installing the Sandtrap software.** We recommend the following installation steps for the USB dongle:

1. Insert the Sandtrap CD in your CD-ROM drive. The USB drivers are on the CD.

2. Plug the dongle into an available USB port.

3. If your system detects the dongle, proceed to step 5.

4. If your system didn't detect the dongle, try rebooting. If it still doesn't detect the dongle, use the Manual Installation steps below.

5. If you are given the option to choose a device type, choose "Other Devices" or "Unknown Device".

6. At the hardware list screen, click on the "Have Disk" button (Windows 98 and 2000 only).

7. Select your CD-ROM drive with the Sandtrap CD in it, as the location of the drivers.

8. Return to the hardware list screen, and choose the appropriate USB Dongle selection for your version of Windows.

9. Proceed with the rest of the installation as prompted by Windows.

Manual Installation: If your system was unable to detect the USB dongle, manually install the driver as follows:

1. Plug the dongle into an available USB port.

2. Open the Control Panel. Open the Add New Hardware or Add/Remove Hardware panel, depending on your system.

3. Follow the steps to add a new device. When you are given the option to choose a device type, choose "Other Devices" (Win98) or "Add a new device" (Windows 2000 and XP).

4. If Windows asks you to either search or select the hardware from a list, choose to select from a list.

5. At the hardware list screen, click on the "Have Disk" button.

6. Select your CD-ROM drive with the Sandtrap CD in it, as the location of the drivers.

7. Back at the hardware list screen, choose the appropriate USB Dongle selection for your version of Windows.

8. Proceed with the rest of the installation as prompted by Windows.

2.5 Uninstalling Sandtrap

To uninstall Sandtrap, click on the **Add/Remove Programs** icon under the Control Panel. Scroll down to the Sandtrap entry, click on the **Remove** button, and confirm your choice.

Because the information in Sandtrap logs may represent weeks or months of work, **log files containing information from Sandtrap are not removed by the uninstaller.** If you wish to remove the Sandtrap logs, you can do so by manually dragging the main Sandtrap directory to the Recycle Bin after uninstalling Sandtrap.

2.6 Reinstalling Sandtrap

Sandtrap does not store its configuration in the Windows Registry. For this reason, the program is relatively resistant to bad interactions with other software or file corruption. Nevertheless, if you have problems with Sandtrap that don't seem related to changes in your hardware configuration, or if the Sandtrap program files become corrupted, you can safely reinstall Sandtrap at any time. You do not need to specifically uninstall Sandtrap before reinstalling it. Note that you cannot reinstall Sandtrap while the previous installation is running.

If you have modified the *sandtrap.ini* file, it will not be overwritten by reinstalling. If you wish to start with a new *sandtrap.ini* file with default settings, move the current one to a different directory or rename it to something else before running Sandtrap the next time. Sandtrap will create a fresh *sandtrap.ini* file with the defaults.

3 Running Sandtrap

Sandtrap monitors modems for incoming telephone calls. Sandtrap can be configured to answer the phone when it rings, or to merely note the Caller ID information. If the phone is answered and Sandtrap is able to negotiate a data connection with the calling computer, Sandtrap will present the caller with a username and password prompt. This information will then be logged using either email alerts or HTTP.

3.1 The Sandtrap User Interface

When you first run Sandtrap, the program will display the Sandtrap monitor window:

```
Sandtrap                                                                 _ □ X
File  View  Tools  Help
11:58:51.4 03fc    OS is Windows 2000 Service Pack 2
11:58:51.5 03fc    Memory in use: 22429696
11:58:51.5 03fc    Mapping modem 1 to port COM1
11:58:51.5 03fc    Mapping modem 2 to port COM2
11:58:51.5 03fc    Mapping modem 3 to port COM3
11:58:51.5 03fc    Mapping modem 4 to port COM4
11:58:51.7 0564    Will answer modem 1
11:58:55.1 0564    Modem 1: Caller-ID enabled
11:59:02.2 0564    Modem 1 ringing; rings received=1
11:59:07.7 0564    Modem 1 ringing; rings received=2
11:59:08.2 0564    Answering modem 1
11:59:26.5 0564    Prompting for username on modem 1
11:59:29.5 0564    Received username 'guest' on modem 1
11:59:29.5 0564    Prompting for password on modem 1
11:59:32.5 0564    Received password 'guest' on modem 1
11:59:34.9 0564    LOGIN ATTEMPTED! (Modem 1) username='guest' password='guest'
11:59:35.1 0564    Will answer modem 1
11:59:38.5 0564    Modem 1: Caller-ID enabled
```

This window allows you to monitor what Sandtrap is doing and to configure Sandtrap's behavior via the **Tools->Options** menu. All information displayed in the monitoring window is saved to the *sandtrap.log* file. All events, such as disabled modems, login attempts, and incoming Caller ID information, are also written to a file called *sandtrap_events.log*.

Sandtrap immediately begins monitoring the modems when you start the program. There is no need to "start" Sandtrap after the program has run. However, unless you properly configure the program, Sandtrap will not actually answer the modems or report intrusion attempts. The configuration information is recorded in the *sandtrap.ini* file. Once Sandtrap has been configured, you can quit the program and restart it without having to re-configure.

3.1.1 Sandtrap's Icon in the Windows Taskbar

In addition to the monitoring window, Sandtrap places the Sandtrap icon (🔺) in the Windows taskbar:
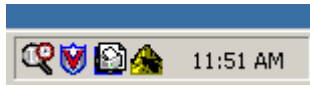
You can access the Sandtrap functions through the pull-down menu options on the monitoring window or by right-clicking on the Sandtrap icon in the taskbar:
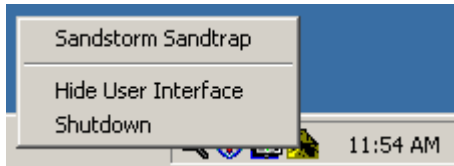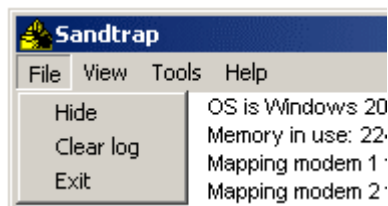
You can also get immediate status information regarding Sandtrap by allowing the mouse cursor to "hover" over the Sandtrap icon:

3.1.2 Sandtrap's File Menu

The Sandtrap File menu is used for the primary control of the interface:

- **Hide:** This option hides the monitoring window. You can make the window reappear by choosing Show User Interface from the Sandtrap icon in the taskbar.

- **Clear log:** This option clears the contents of the monitoring window. The *sandtrap.log* file is not affected.

- **Exit:** This option closes the monitoring window and causes the Sandtrap program to exit.

3.1.3 Sandtrap's View Menu

The Sandtrap View menu allows you to control options on the Sandstorm user interface.
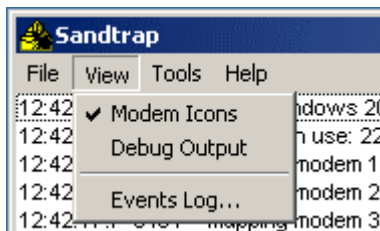
- **Modem Icons:** Selecting this option causes Sandtrap to display indicator icons in the Windows task bar for each modem that is licensed. For example, if you select this option and have three

16

modems that are disabled, Sandtrap will display:

- **Debug Output:** Selecting this option causes Sandtrap to display more detailed information in the monitor window.

- **Events Log…** Selecting this option causes the current contents of the file S*andtrap_Events.log* to display, using the Windows Notepad application. This provides an easy way to see a log of just the events that have happened up to the time of the display, such as login attempts, disabled modems, and incoming Caller ID information. You can designate a different viewer application, as well as elect to include dates in the events log filename, on the Logging tab of the Sandtrap Properties window. See the *Setting Up Sandtrap* section for further information.

3.1.4 Sandtrap's Tools Menu

The Sandtrap **Tools** menu allows you to control the behavior of the Sandtrap application.
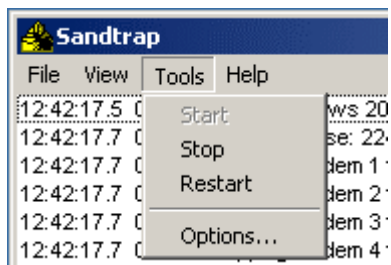
- **Start:** Normally, Sandtrap starts monitoring the modems when you start the program. If you had previously selected **Stop** to stop monitoring, selecting **Start** will resume monitoring.

- **Stop:** Selecting **Stop** will cause Sandtrap to stop monitoring the modems.

- **Restart:** Selecting this option is the same as manually selecting **Stop** and then **Start**. Normally you do not need to use the **Restart** option, but if you are having problems with your Sandtrap modems, you may find this option useful.

- **Options…** This menu option brings up the Sandtrap Properties configuration window. See the *Setting Up Sandtrap* section for further information.

3.1.5 Sandtrap's Help Menu
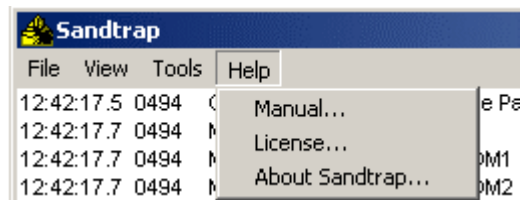
- **Manual…** This displays the online version of this manual, using HTML Help.

- **License…** This option displays the Sandtrap End User License Agreement.

- **About Sandtrap…** This option displays information about the current version of Sandtrap.

To assure yourself of the accuracy and reliability of the data collected using Sandtrap, you should run a test from a known number using a utility like Hyperterminal. See the *Sandtrap QuickStart* document for test instructions.

3.2 Setting Up Sandtrap

The Sandtrap Properties configuration window is accessible from the **Tools->Options** menu. There are three tabs in the properties window:

- **Modems:** Allows configuration of individual modems.

- **Alerts:** Allows you to enable, disable and configure SMTP and HTTP alerts.

- **Emulation:** Allows customization of the banner, login prompt, password prompt, and login failure message that any modem dialing into Sandtrap will see.

- **Logging:** Allows you to designate a viewer for the events log, and use a unique events log file name for each day that you start Sandtrap.

3.2.1 Modems Tab
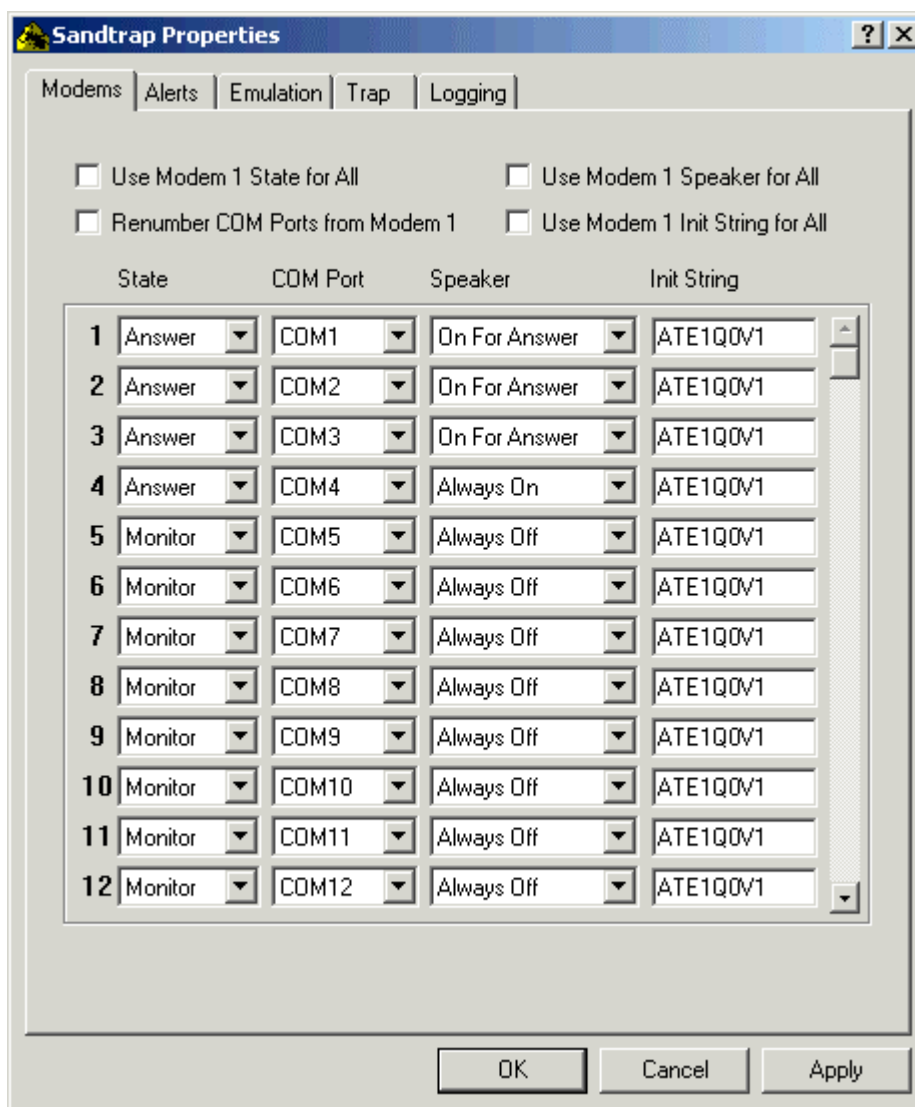
The number of modems you can use with Sandtrap is contained in the hardware license manager. If you have many modems that will be using the same settings, use the convenience options at the top of the **Modems** tab:

- **Use Modem 1 State for All:** When checked, the State setting for Modem 1 will be used for all modems.

- **Renumber COM Ports from Modem 1:** When checked, COM ports for all modems will be set in sequence starting at the COM port for Modem 1. COM port renumbering stops at COM 255.

- **Use Modem 1 Speaker for All:** When checked, the Speaker setting for Modem 1 will be used for all modems.

- **Use Modem 1 Init String for All:** When checked, the Init String setting for Modem 1 will be used for all modems.

There is also a row of fields for each modem.

- **Number:** The number of the modem. This is the same number that appears in each modem indicator icon in your Windows taskbar.

- **State:** The modem state may be Off, Answer, or Monitor. Monitoring modems will log Caller ID information but will not answer.

- **COM Port:** The COM port the modem is attached to. Consult your Windows Device Manager settings, or run *checkmodems.exe* to see which COM ports your modems are connected to.

- **Speaker:** The modem's speaker may be Always Off, Always On, or On For Answer (off once the connection is established).

- **Init String:** A command string sent to the modem during initialization. In most cases this will not need to be changed. If it is necessary, consult your modem hardware documentation to determine the correct init string.

3.2.2 Alerts Tab

The **Alerts** tab contains configuration for SMTP and HTTP alerts, which can be sent out when certain Sandtrap events occur, such as a login attempt. You can elect to use one, both, or neither alert method. All events, even if alerts are not enabled, are recorded in the *Sandstorm_Events.log* file. These alerts will be sent when Sandtrap events occur for the selected Alert Types:

- **Answer:** When the modem answers, it will send an alert with the date and time.

- **Caller ID:** When Caller ID information is received by a listening modem, it is included in the alert with the date and time.

- **Login Attempt:** When checked, alerts will be sent containing information about a login attempt. This includes the date and time of the attempt, and the username and password used in the attempt.

- **Trap Mode:** When checked, an alert will be sent whenever any modem goes into Trap mode. See **Section 3.2.6** for a description of Trap mode.

- **Modem Disabled:** If a modem becomes disabled during monitoring, Sandtrap sends an alert with the date and time, which modem, and why it was disabled.

- **Shutdown:** An alert is sent out if the Sandtrap program is shut down, containing the date and time the shutdown occurred.

3.2.3 Alerts Tab: SMTP Settings

SMTP alerts can be sent to email accounts or pagers. The default settings can be customized for your company's information or mail filtering.

- **Enable SMTP Alerts:** When checked, SMTP alerts will be sent for all of the Alert Types that are checked. If not checked, the following SMTP settings will be grayed out.

- **To address:** This is the email address to send SMTP alerts. This field is required.

- **Cc address:** This is the email address to send a carbon copy of SMTP alerts.

- **Bcc address:** This is the email address to send a blind carbon copy of SMTP alerts.

- **From address:** This is the email address the SMTP alerts will appear to be sent from.

- **Subject line prefix:** The subject line for SMTP alerts will consist of this prefix, followed by the alert type.

- **Outgoing mail (SMTP) server:** The outgoing mail server to use for SMTP alerts. This field is required. Ask your system administrator, or you can use the same outgoing mail server that your default email program uses.

3.2.4 Alerts Tab: HTTP Settings

HTTP alerts are sent to web servers. Sandstorm provides an unsupported sample web server called the Sandstorm Alert Manager (*sam.exe*), along with a sample web page (*default.html*) and CGI script (*psalert.cgi*).

- **Enable HTTP Alerts:** When checked, HTTP alerts will be sent for all of the Alert Types that are checked.

- **URL:** Where to send the HTTP alert. This field is required. For example, if you are using a CGI script called *psalert.cgi* on a local web server, you would use something like: http://localhost/cgi-bin/psalert.

- **Username:** If your web server requires a login, the username goes here.

- **Password:** If your web server requires a login, the password goes here.

- **Extra arguments:** Any extra arguments that would be sent, for example to a CGI script. An example would be *color=red* if your CGI script uses a text color for an alert.

3.2.5 Emulation Tab

Using the **Emulation** tab, you can customize the information that a caller will see when they attempt to login to Sandtrap. This allows you to emulate a specific system, or present information required by your company. It also allows you to control how long Sandtrap will wait for a connection or responses to prompts. Emulation can be set per-modem. Default settings are provided as an example.

Each setting (except the response timeout) can be one or more lines, or can even be blank.

- **Banner:** One or more lines of introductory text presented before the login prompt.

- **Display Between Login Tries:** When checked, the banner will be redisplayed between multiple login tries.

- **Login prompt:** This prompts the caller to enter a user name.

- **Use:** When checked, the login prompt will be used. When unchecked, Sandtrap can emulate systems that present a password prompt only.

- **Password prompt:** This prompts the caller to enter a password.

- **Failed password message between multiple login tries:** This informs the caller that the login attempt failed, if there are multiple **Login Tries** set. The banner (if the **Display Between Login Tries** banner option is checked) and the username prompt appear after this message is displayed.

- **Message at end of call:** This informs the caller that their login attempt failed and that the connection is being terminated.   Sandtrap hangs up the call after this message is sent.

- **Login Tries:** This is how many times Sandtrap will prompt for a username and password, before the end of call message is displayed.

- **Modem:** Each modem can answer with different emulation settings. This drop-down list selects the modem this group of settings corresponds to.

- **Response Timeout (seconds):** This is how many seconds Sandtrap will wait for a response from the other modem when answering, prompting for login, or prompting for password. If the timeout is reached without a response, Sandtrap will hang up.

- **End of call Timeout (seconds):** This is how many seconds Sandtrap will wait after the last failed password attempt, before hanging up.

- **Use Defaults:** This sets all visible emulation settings to the Sandtrap defaults. Click the **OK** or **Apply** button to apply the settings.

- **Use these settings for all modems:** When checked, the currently visible settings will be used for all modems when the **OK** or **Apply** button is clicked.

3.2.6 Trap Tab

The **Trap** tab allows you to put a modem into an interactive "trap" mode at the specified stage of a call. In trap mode, Sandtrap will not hang up the modem until it is manually reset. This is useful for keeping the line open for call tracing, and for providing more extensive emulation. An alert will be sent upon entering trap mode, if alerts are enabled and the **Trap Mode** box is checked on the **Alerts** tab. The modem can be reset by right-clicking on the modem icon and choosing **Reset** from the popup menu.
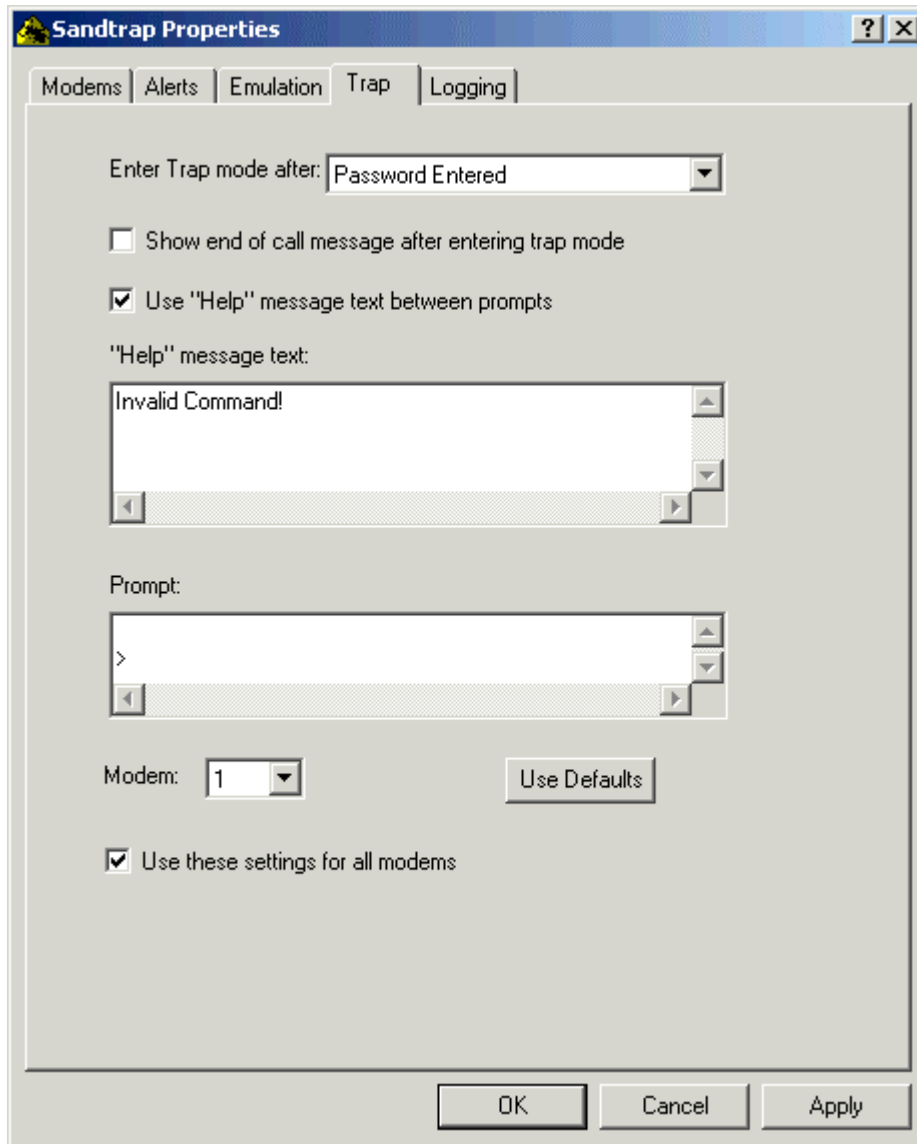
The following settings can be changed on this tab, on a per-modem basis:

- **Enter Trap Mode after:** Trap mode will be entered for this modem in the following stage of a call: Never, after answer, after the username is entered, or after the password is entered.

- **Show end of call message after entering trap mode:** Sandtrap can display the end of call message (set on the **Emulation** tab) upon entering trap mode. When using this option, you may wish to change the end of call message to indicate successful penetration of the emulated system.

- **Use "Help" message text between prompts:** In trap mode, Sandtrap will present the caller with a prompt after each carriage return the caller enters. When this box is checked, Sandtrap will also display an additional message before each prompt. This allows emulation of a help or error message from the system.

- **"Help" message text:** Text presented to the caller after each carriage return entered, if the Use "Help" message text box is checked.

- **Prompt:** Characters presented to the caller after each carriage return entered in Trap mode. You may wish to customize this to a typical prompt for the system Sandtrap is emulating.

- **Modem:** Each modem can enter trap mode at different times or not at all, and use different prompt sets. This drop-down list selects the modem this group of settings corresponds to.

- **Use Defaults:** This sets all visible Trap mode settings to the Sandtrap defaults. Click the **OK** or **Apply** button to apply the settings.

- **Use these settings for all modems:** When checked, the currently visible settings will be used for all modems when the **OK** or **Apply** button is clicked.

3.2.6.1 *Sample Trap Session*

This is a sample session of a caller dialing into a Sandtrap modem in trap mode. The end of call message on the **Emulation** tab has been changed to a welcome message.

```
ATDT5551234

CONNECT 9600

Remote Access Service.
UNAUTHORIZED USE PROHIBITED.
Login: root

Password:

Welcome to the XYZ Company System!

> help

Invalid Command!

> dir

Invalid Command!

> quit

Invalid Command!
```

3.2.7 Logging Tab

The **Logging** tab allows you to control how you view the Events Log from within Sandtrap, and provides the option to automatically create a new dated events log for each day that you start Sandtrap.
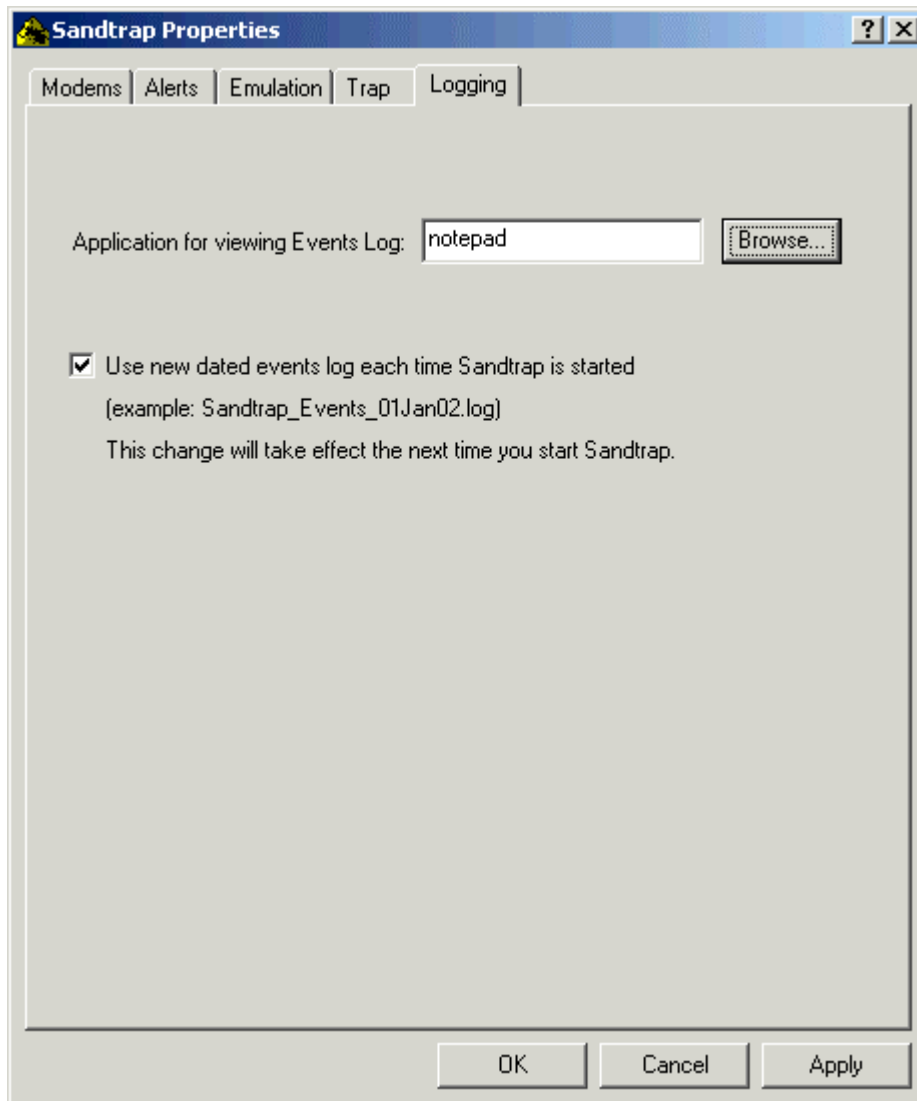
The following settings can be changed on this tab:

- **Application for viewing Events Log:** This is the application that will be called by Sandtrap to display the current contents of the events log. The default is Notepad. If you use a different application, make sure it is either in your PATH or that you provide a full path name (e.g. *C:\apps\myreader.exe*). You can also use the **Browse** button to find and select an application.

- **Use new dated events log each time Sandtrap is started:** When this is checked, each time you start Sandtrap the events log file name will include the date. An example is *Sandtrap_Events_01Jan02.log*. This allows you to easily archive your event logs. If you start Sandtrap multiple times in the same day, log information will be appended to the same file for

that day. If this option is not checked, the file *Sandtrap_Events.log* is used. Changing this setting takes effect the next time you start Sandtrap.

3.2.8 Sandtrap.ini file

Sandtrap can also be configured by directly editing the *sandtrap.ini* initialization file. If you choose to do so, you must restart Sandtrap after editing the file for the changes to take effect. The items in *sandtrap.ini* correspond directly to the settings on the **Sandtrap Properties** window tabs.

3.3 Before You Start

- Verify that the hardware license device (dongle) is connected to your computer's parallel or USB port and seated firmly. You can run Sandtrap for 5 minutes without a dongle; after that Sandtrap will quit.

- Disable any fax or remote access software that uses the same modems or COM ports as Sandtrap, including PhoneSweep.

- Disable your computer's power management software and/or screensaver.

- On Sandtrap's properties window (off the **Tools->Options** menu) on the **Modems** tab, make sure you have assigned the correct COM port and answer state for your modem(s). Modems can be in either Monitor or Answer state. Monitor state means that the modem will record Caller ID information, but will not answer.

- On Sandtrap's properties window, select the **Alerts** tab and make sure you have enabled the desired alert options and provided necessary information (such as your email address and outgoing mail server, for SMTP alerts).

- On Sandtrap's properties window, select the **Emulation** tab and make any desired customizations to the banner, login and password prompts, and failed login message that callers will see.

3.4 During the Monitoring Process

While Sandtrap is running, it is always monitoring, unless you have told it to **Stop** or all modems are disabled. If you use the Sandtrap Properties window to change options, Sandtrap resets and starts monitoring again after you apply the changes.

You can tell what is going on during the monitoring process in several ways:

- **Modem Indicator icons:** These appear in your taskbar icon tray, and there is one for each modem. The icons will have a gray background if the modem is disabled, a black background if it is idle or monitoring, and a red background if it is answering an incoming call. Each indicator icon has a status tooltip, which appears when you run the mouse over the icon. This tooltip is useful for determining what the modem is doing at a given time.

- Each indicator also has a right-click popup menu. Using this menu, you can disable individual modems, or attempt to reset them if they have become disabled or inactive.
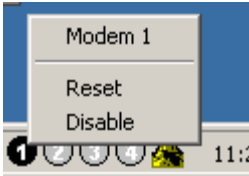
- **Sandtrap main window:** A scrolling, time-stamped log of activity appears on this window. Everything appearing here is also saved in the file *sandtrap.log*. You may wish to save copies of *sandtrap.log* periodically for audit and archive purposes, or to send to Sandstorm Support to report a problem. The events log file (*Sandtrap_Events.log*) contains a subset of this information including login attempts and Caller ID info, which is useful for a quick review.

- **View -> Events Log:** This shows the current contents of the events log file up to the time that it is displayed. You will need to close and redisplay it to get more events.

- **SMTP or HTTP alerts:** Sandtrap will send SMTP and/or HTTP alerts, as desired. You can configure these on the Alerts tab, on the Sandtrap Properties dialog. This allows you to receive email or pager alerts, or direct alerts to a web server. An unsupported sample web server, the Sandstorm Alert Manager, is provided with Sandtrap as an example. All events that can be sent as alerts are also recorded in the file *sandtrap_events.log*, whether or not alerts are enabled.

An example of a typical SMTP login attempt alert email:

```
From:      Sandtrap-alerts@sandstorm.net
To:        me@mycompany.com
Cc:        boss@mycompany.com
Subject:   SANDTRAP ALERT:  Login Attempted.


Fri Jan 04 09:49:16 2002


Login Attempted.
Modem 1
username: myuser
password: rover
```

An example of a typical SMTP Caller ID alert email:

```
From:      Sandtrap-alerts@sandstorm.net
To:        me@mycompany.com
Subject:   SANDTRAP ALERT:  Caller ID


Fri Jan 04 17:23:55 2002


Caller ID
Modem 1
DATE = 0104
TIME = 1720
NAME = MR_HACKER
NMBR = 6175551234
```

3.4.1 Why might a modem become disabled?

A modem is always disabled if its state is "Off" on the **Modems** tab. It may also become disabled if Sandtrap cannot communicate with it. If this happens, make sure you have the right COM port assigned to the modem, and that the modem is powered on.

Appendix A: Glossary

Administrator: On Windows NT, 2000, and XP, the level of privilege that allows users write access to all files, to install new services, and to create new users. Analogous to *root* on a UNIX system. Because the hardware management device services must be installed, an Administrator user on Windows NT/2000/XP must install Sandtrap.

Bi-directional parallel port: A parallel port that can be written to as well as read from. Devices attached to a bi-directional parallel port can both receive input from the computer and return status information.

BIOS: Basic Input/Output System. The ROM code that runs on startup and communicates with hardware to load the operating system.

checkmodems.exe: A program in the top-level Sandtrap directory that identifies modems and their COM ports, and determines if they are connected properly to a phone line.

CMOS: Complementary-symmetry Metal Oxide Semiconductors. Non-volatile memory that records BIOS settings when a machine is powered off.

COM port: another name for a serial port. Knowing which COM: ports your modems are connected to is important for configuring Sandtrap.

Data communications: The exchange of information by two modems; communications that are not fax communications.

Data device: A device that is capable of being a modem.

DB9: A type of serial port connector with 9 pins in a D-shaped shell. Normally used for RS-232 serial communications. Compatible with 25-pin DB-25 cabling with proper adapter connectors.

Desktop: The main Microsoft Windows window (or view).

Dongle: Another term for Hardware License Management Device. When attached to a computer's parallel or USB port, allows Sandtrap to answer actual calls. The dongle prevents pirated copies of Sandtrap from being misused.

Hardware License Manager: A device that must be connected to the parallel or USB port of a computer running Sandtrap before Sandtrap will listen for calls. Also called a "dongle".

hhupd.exe: A program in the top-level Sandtrap directory that installs HTML Help on a computer that does not already have it.

I/O address: Associated with IRQs, an I/O address is internal to the computer and is used to communicate with a specific device.

Initialization string: A command sent to a modem before Sandtrap puts it into listening mode.

IRQ: Interrupt Request. Hardware devices use IRQs to request service from the operating system when I/O operations complete or there is new data to be processed. If the operating system is not configured to know which devices are using which IRQ lines, it may crash, or the devices may be unusable.

PCMCIA: Personal Computer Memory Card Internal Association. Also called "PC cards." A credit-card sized I/O device for laptop computers - may provide a network adapter, modem, or multiple RS-232 serial ports.

Remote modem: A modem that dials into Sandtrap.

Response string: The characters sent by Sandtrap when it answers an incoming call.

Serial port: An I/O device that sends and receives data bytes over an RS-232 serial line. Used to connect modems and sometimes printers to PCs.

Sleep Mode: A power-saving mode implemented by some desktop and laptop computers. If disk and communications activity only will not prevent the computer from entering sleep mode, then sleep mode must be disabled before leaving Sandtrap running unattended.

Tab: An area on the Sandtrap Properties dialog that can be selected to reveal a set of related information or configuration options.

TAPI: Microsoft's Telephony Application Programming Interface.

Testing injury: An undesired result of running Sandtrap, such as accidentally sending email alerts to the wrong address. The Sandtrap license agreement explicitly states that the end user assumes all liability for any testing injuries.

Unsecured modem: A modem connected to a system that allows login without a password or with an easily guessed password.

USB interface: Universal Serial Bus. A serial I/O channel to which multiple peripherals can be connected, most commonly found in laptops.

Appendix B: Sandtrap FAQ

The Sandtrap FAQ is a collection of Frequently Asked Questions and answers about normal Sandtrap operations. For information on diagnosing problems and troubleshooting, please see Appendix C: Sandtrap Troubleshooting Guide.

Using Sandtrap

Do the modem drivers need to be installed for Sandtrap to work?

No. Sandtrap uses the low-level COM port drivers instead of TAPI.

Will HTML Help run if the computer running Sandtrap does not have Internet Explorer installed?

Probably yes, if you run *hhupd.exe* in the top level Sandtrap directory. Note, however, that having IE installed on a computer does not mean that you have to use IE at all; you can keep running your preferred web browser.

Can I use Sandtrap with Remote Software?

We have performed some testing with Sandtrap with PCAnywhere and NetOp, but we cannot guarantee 100% compatibility. Make sure such software loads and operates correctly on its own before you attempt to use Sandtrap over it.

Appendix C: Sandtrap Troubleshooting Guide

This section contains information that can help resolve problems that crop up in the course of running Sandtrap. **Please read this section before contacting Sandstorm Technical Support.** Many problems have uncomplicated solutions, and this section will usually give the quickest way to get Sandtrap up and running again.

This section is divided up into several subsections:

- Information you should have available while troubleshooting Sandtrap.

- Easily rectifiable situations that may cause problems running Sandtrap.

- Common problems encountered while running Sandtrap and possible solutions for them.

- Error messages, their causes and possible solutions.

- Other things to try.

Information To Collect Before Troubleshooting

- **Error Messages**: Make a note of any error messages, *including their exact text.* Error messages may appear in dialog boxes and can also be viewed in the files *sandtrap.err, sandtrap.log,* and *sandtrap.log.bak*.

- **Operating System**: What version of Windows is Sandtrap being used with? Some problems are OS-specific.

- **Modem**: What brand and model of modem was Sandtrap using to dial? What does *checkmodems.exe* say about your modem? Many problems can result from using a misconfigured or non-recommended modem, because Sandtrap's performance depends heavily on the modem. **If *checkmodems.exe* can find your modems, but Sandtrap cannot, have you set the correct COM port for your modem in Sandtrap?**

- **Phone System / PBX**: What make/model phone system / PBX are you using?

- **Version number**: What version of Sandtrap was having problems? Often, bugs found in older versions of Sandtrap will have been corrected in subsequent releases.

- **What changed since things last worked?** When Sandtrap "just stops working," the reason is usually a side effect of some other change to the computer or its environment. Check your modem cables, telephone jacks and the software environment (O/S changes, new applications using the COM port, internal security software, etc.). Also, ask your telecommunications service if they have performed any work on the phone system that might have affected Sandtrap.

Things To Check If You're Having Trouble

- **Are you running Sandtrap with a non-recommended modem**? The quality of the information collected by Sandtrap depends heavily on the modem used. For example, a modem that does not support Caller ID will result in no Caller ID alerts. Try using a recommended modem. The updated list is at http://www.sandstorm.net/products/phonesweep/reccmodems.shtml.

- **Did you manually lock the computer while Sandtrap was running?** Using a software screen-locking tool to manually lock the computer running Sandtrap can cause problems. Try unlocking the computer and restarting Sandtrap. If this is the problem, and you need to lock your screen, we recommend the third party product, ScreenLock, which can be run on Windows 95, 98, NT 4.0, 2000, and XP. You can obtain it from http://www.screenlock.com.

- **Was a screensaver or other software (such as a virus checker) running simultaneously with Sandtrap?** Try disabling the screensaver or other software and restarting Sandtrap. If this does not work, disable all non-essential software before restarting Sandtrap. If you need to be able to lock your screen, use ScreenLock, which can be obtained from http://www.screenlock.com.

- **Is the hardware license manager attached to the parallel or USB port and firmly seated?** You can run Sandtrap for 5 minutes without a hardware license manager; after that Sandtrap will quit. If the license manager disengages from the parallel or USB port while Sandtrap is running, Sandtrap will stop monitoring. Reattach the license manager and restart Sandtrap. If you are using Windows NT, you may need to reboot your PC.

- **Are you running Sandtrap on a laptop running on battery power?** The laptop may not automatically activate the port that the dongle is plugged into. If you can't plug in the laptop, attach a device with an independent power supply, such as a printer or fax machine, to the dongle and restart Sandtrap.

- **Are you running Sandtrap on a laptop with Windows NT?** Sandtrap works best on laptops that are running Windows 98, 2000, or XP. If you have the option of running Sandtrap under one of these operating systems, do so.

- **If you are running Sandtrap under Windows NT, 2000, or XP, was the dongle attached to the parallel or USB port and firmly seated during installation?** The dongle must be attached during the install for Sandtrap to install correctly. If the hardware license manager was not attached to the correct port during the Sandtrap installation, attach the hardware license manager to the correct port and follow the directions in Section 2.4,

Hardware License Protection, to reinstall Sandtrap.

- **If you are running Sandtrap under Windows NT, 2000, or XP, were you logged in as an Administrator when Sandtrap was installed?** To run correctly under Windows NT/2000/XP, an Administrator must install Sandtrap.

- **If you are running Sandtrap on Windows NT, do you have write permission for the Sandtrap directory?** If you want to run Sandtrap as a non-administrator, Sandtrap must be able to write to its log files. An NT Administrator can reset the Security values under the Properties of the Sandtrap directory.

  If you are running Sandtrap under certain Windows NT configurations or security settings, it is possible that Sandtrap may need to be run by an Administrator. Doing so will guarantee Sandtrap access to the files, devices and system services it requires.

- **Did you copy missing DLL files from another computer?** Copying DLL files from one computer to another does not work. If you are running Sandtrap on a Windows NT system and you get an error message stating that you are missing DLL files, try installing Internet Explorer 4.01 or higher, and upgrading to a newer NT service pack.

- **Do you already have another copy of the Sandtrap engine or database running?** Hit CTRL-ALT-DEL to bring up the Task Manager and kill any processes named Sandtrap and restart Sandtrap.

- **Does the computer on which you are running Sandtrap meet the system requirements?** See Section 2, Installation and Setup.

- **Is any other software running simultaneously with Sandtrap?** In rare instances, some software may conflict with Sandtrap, most often when attempting to share COM ports. Try shutting down all other programs and restarting Sandtrap. It has also been reported that having Norton Autoprotect installed on a computer can cause a general protection fault when the Sandtrap InstallShield installer is running.

Common Problems and Possible Solutions

- **Sandtrap will not start monitoring**. If you click on Start and Sandtrap does not begin monitoring, first collect some information and refer to the more specific situations below. Make sure the dongle is attached and firmly seated, the modems are turned on, at least one modem is selected on the **Modems** sub-tab, and the COM ports do not have any IRQ conflicts.

- **Sandtrap stops monitoring.**
  - Check to see if the hardware license management device has become loose or disconnected from the computer's parallel or USB port.
  - Do you have other software running on the computer? Try disabling all other software before running Sandtrap. Contact Sandstorm if this does not work.

- **No Caller ID information is being recorded.** Your modem may not support Caller ID mode. Check with the modem manufacturer, or use one of Sandstorm's recommended modems listed at http://www.sandstorm.net/products/phonesweep/reccmodems.shtml.

- **HTML Help doesn't work**. Try running the HTML Help installer *hhupd.exe* in the top-level Sandtrap directory. If this doesn't work, try installing Internet Explorer 4.01 or 5.0 on your computer or, on an NT system, upgrading to a newer service pack.

- **Sandtrap reports that a DLL file is missing**. Copying DLL files from one computer to another does not work. Installing Internet Explorer 4.01 or higher and reinstalling Sandtrap may clear up the problem. Upgrading the service packs may help; there may be a way to get DLL files from the NT service packs.

- **Sandtrap stops working after an NT workstation upgrade**. This is likely a Microsoft problem; installing Internet Explorer 5.0 may clear up the problem.

- **Running a screensaver makes Sandtrap lock up**. Unfortunately, there is currently no way to ensure that Sandtrap will run correctly if a screensaver is running at the same time. There is no way to predict whether Sandtrap will or will not have problems with a given screensaver. Disable the screensaver if it appears to be causing problems. We have tested a third party product called Screen Lock. It works on Windows 95, 98, NT, 2000, and XP and allows you to run Sandtrap and other programs in the background. You can obtain it from http://www.screenlock.com.

- **A multi-port serial card does not work.** Resetting the cards and connections is a good place to start. If you have multiple cards, try swapping them, and/or swapping their cables. If nothing else works, uninstall the cards and drivers and start over.

- **Reseating the multi-port serial card or its cable several times still doesn't get the computer to acknowledge the card.** It is possible that the card and/or cable are defective. If possible, try to install the card on another machine, preferably one with different hardware or operating system. If you are able to install the card on another machine, have your company's technical support personnel check your own machine's settings. After testing, if it appears that the card and/or cable are defective, call the manufacturer. If you bought the card from Sandstorm, please call our Technical Support department.

- **I installed a multi-port serial card, but I cannot set my UART's or COM ports for modems.** Some machines (especially Dell Optiplexes) are picky about where you place multi-port cards. If you are using a SeaLevel card on a Dell Optiplex, try moving it to the middle port. On other machines, move the card to the port normally used by the internal modem (this usually maps to COM 2 or 3).

- **I added a multiport serial card, but fewer COM ports are visible in software than I expected**. Remove the card and reboot the computer, and see if the number of COM ports increases. If not, you may have a resource conflict. Try re-installing the hardware and drivers.

- **I am using an 8-modem card, but only COM ports 5-10 are found**. On some systems, you may need to manually install the modem drivers on COM ports 11 and 12).

- *checkmodems.exe* **is not identifying the devices on the COM ports correctly**. Check the settings in the Device Manager and ensure that they are correct. If this is not the problem, try one of the following:

   o Turn the modem(s) on and off; reseat all connections involved.

   o Swap modems and cables (and multi-port serial cards if you are using them) to see if the problem is associated with a particular piece of hardware.

   If the problem follows a particular piece of hardware, or you cannot fix it, contact the manufacturer or Sandstorm Technical Support if you purchased your modems from us.

- *checkmodems.exe* **hangs at one port.** Try resetting the modem at that port, and reseating its cable. Try swapping cards and/or cables if you are using a multi-port serial card.

- *checkmodems.exe* **finds the Modems, but Sandtrap does not (when I check under the Modems sub-tab, the COM Ports are wrong).** When running *checkmodems.exe*, note what

COM ports the modems are actually on. Then, go to the **Modems** tab, and click the drop down list under the COM Port column for the modem in question. This brings up a pull-down menu where you can select the correct COM port for each modem. Once you save any changes, Sandtrap will find the modems. If Sandtrap continues to give you problems after this, please call Sandtrap Technical Support.

Sandtrap Error Messages

Error messages on install

- **"Move data error":** This error indicates a problem with the installation CD-ROM itself. The CD-ROM could be scratched or have a defect that was not spotted during testing. If you encounter this error, contact Sandstorm Enterprises and request a replacement CD-ROM. In rare cases, it may turn out that the manner in which the data is burned onto the CD-ROM is not compatible with your CD-ROM drive. Installing Sandtrap by copying files from another computer may help, or Sandstorm may be able to help devise a workaround.

- **"The file *filename* is locked and not writeable":** During an installation, this means that some part of Sandtrap was running and could not be overwritten. If the Sandtrap User Interface is running, shut it down before attempting the install. If the debugging file *debug.bat* is running, close the DOS window it is using. If neither of these are running, hit CTRL-ALT-DEL to bring up the Task Manager and kill any processes named <u>Sandtrap</u>. Alternatively, you can reboot your computer and begin the install again.

- **"Sandtrap requires Administrator privileges on Windows NT"**: This indicates that you are installing Sandtrap on a Windows NT system, but you do not have administrative privileges. Because Sandtrap must install a service to interface with the hardware license manager, it must be installed by Administrator on Windows NT.

- **"d:\setup.exe not a valid NT program**.": Make sure you've selected the CDROM drive, and that it contains the Sandtrap CD.

Error messages for individual modems

- **"Disabled: <error message>":** Follow the steps below to diagnose the problem:
  - The error message will tell you why Sandtrap was not able to use this modem. Check the main Sandtrap window or the *sandtrap.log* file to determine the exact error message.
  - There may be a problem with your computer's COM ports. Run *checkmodems.exe* to test your COM ports.
  - The modem may not be turned on or plugged in. Make sure that the modem is turned on and plugged firmly into a valid analog phone line. Remember that analog modems will not work when plugged directly into a digital phone line. If you have multiple modems and one is working, switch the working modem's phone line with the problem modem's phone line. If the previously working modem then experiences problems, the problem is with the phone line.
  - Many modems have two RJ11 backs on the back, one to hook into your phone system, one for an optional handset. Be sure you are using the proper jack, usually labeled "LINE."
  - There may be physical problems with the modem itself. If applications other than Sandtrap cannot use the modem, the modem may be broken or defective, or incorrectly cabled.

- If some modems connected via a Quatech PCI card stop working when the modems are moved around, check the connectors to see if they are loose. The connectors do not have screws to secure them to the modems.

- **"Cannot open COM: <number>":** This message usually means either that the PC does not have that COM port installed or that some other application is currently using that particular COM port. Run *checkmodems.exe* to further diagnose the problem.

I've Tried Everything and Sandtrap Still Doesn't Work!

First, check all the cables to the modems, and the phone jack wires that connect the modems to the phone lines. Make sure your modems are powered on. Second, reboot your PC. Windows itself can become unstable and cause problems for applications trying to run under it. If you are running Sandtrap under Windows 95 or NT, try running Sandtrap under Windows 98, 2000, or XP instead. Users have historically reported fewer problems running Sandtrap under Windows 98/2000/XP than under Windows 95 or NT. If you are still having problems, contact Sandstorm Technical Support.

Appendix D: Important Web Sites and Phone Numbers

Sandstorm Enterprises (617-426-5056): http://www.sandstorm.net

> Recommended Modems:
> http://www.sandstorm.net/products/phonesweep/reccmodems.shtml

> Recommended Serial I/O cards:
> http://www.sandstorm.net/products/phonesweep/multiport.shtml

Multiport Card Vendors

SeaLevel (SeaLevel VersaCom +4 (7401) and +8 (7801)Serial I/O multiport cards, and SeaPort +4/232 (2401) box): http://www.sealevel.com

Installation Note: You must first install asynchronous drivers before installing serial I/O card and attach the octopus cable. IMPORTANT: If you are putting your multiport card on a Windows 2000 system, go to the SeaLevel website to get the **latest** drivers. Pre-January 2001 drivers can cause the system to freeze.

4 port cards: http://www.sealevel.com/catalog/4portpcia.htm

8 port cards: http://www.sealevel.com/catalog/8portpcia.htm

SeaPort USB to 4-port Serial box: http://www.sealevel.com/catalog/2401.htm

Drivers: http://www.sealevel.com/catalog/asyncsw.htm

Quatech (Quatech QSP 100 4 port PCMCIA serial I/O adaptor with cable for laptops)
> http://quatech.com

Modem Vendors

Zoltrix (Zoltrix Rainbow 56K modem, FM-VSP56e2 and FM-VSP56e3)
> http://www.zoltrix.com or http://www.zoltrix-int.com (International Web Site)

> Installation notes: Sandtrap does not use the drivers that come with your modem. However, to prevent the Add New Hardware wizard from coming up every time you restart your PC or laptop, we recommend that you install the modem drivers, then turn them off under Modem Properties in the System Devices panel found under Start->Settings->Control Panel. Sandstorm does sell Rainbow Modems if you are unable to find a nearby modem supplier in the U.S..

Multi-Tech: (Multi-Tech Systems MultiModem 56K Voice/Data/Fax (Multi-Tech MT5600ZDXV)
http://www.multitech.com
(http://www.multitech.com/PRODUCTS/MultiModemZDX)

For ISDN: US Robotics External Courier Imodem: http://www.usr.com. Note: Site uses Java.

ScreenSaver Vendor

ScreenLock: (ScreenLock, password protection/screen saver that allows programs to run in the background. Tested and approved for use with Sandtrap):
> http://www.screenlock.com

Appendix E: Contacting Sandstorm

This appendix describes how to contact Sandtrap technical support and sales. We're always glad to hear from you. **Your comments are valuable to us.** By telling us what features you want to see in Sandtrap and working with us to resolve problems, you can help us deliver a product that lives up to your expectations.

About Technical Support for Sandtrap

Sandtrap comes with 60 days of free Support/Update service. You can purchase 12-month extensions of your Support/Update service either with your initial purchase of Sandtrap, or later. If Sandstorm releases a new version of Sandtrap during the period of your Support/Update contract, you will automatically receive the new version free of further charge.

Submitting Bug Reports

A Support/Update service contract is <u>not</u> required to submit bug reports. If you believe you have found a bug, please let us know so that we can fix it and deliver a better product. Sandstorm provides a web form at http://www.sandstorm.net/support for convenient submission of bug reports.

Before You Contact Sandstorm Technical Support

Before contacting Sandstorm Enterprises Tech Support, please follow these two steps:

Look through Appendix C: Sandtrap Troubleshooting Guide. The Troubleshooting Guide contains a clear summary of many common problems with Sandtrap and their solutions.

Have the following information readily available:

- Version number of your copy of Sandtrap. See the Help/About button in the main Sandtrap window.

- What platform you were running Sandtrap on at the time of the problem, including Operating System version and Service Pack level.

- The brand and model of the modem you were using.

- The CPU speed of the computer that had problems running Sandtrap.

- The amount of RAM in the computer that had problems running Sandtrap.

- Any error messages that Sandtrap displayed at the time the problem occurred (Please try to get exact wording, as this can indicate the source of the problem).

- Also the Make/Models of any Multi-port and/or Network cards.

- Did Sandtrap work on the same machine prior to this? Did something change?

Save the files *sandtrap.log* and *sandtrap.log.bak* (if it exists). Although we may not ask for it right away (it can be a very large file) we may request that you send it to us later for debugging purposes.

Contacting Sandstorm Technical Support

On the web: Go to http://www.sandstorm.net/support. The technical support web page contains an automated system for asking technical questions and submitting bug reports.

By email: Send email to support@sandstorm.net.

By phone: You can reach Sandstorm Enterprises at (617) 426-5056. We are generally available to answer technical support questions between the hours of 9:00 AM and 5:00 PM US Eastern Time (GMT minus 5:00).

Contacting Sandstorm Sales

For pre-sales assistance, information about future versions of Sandtrap, or to order products from Sandstorm, you can reach us in three ways:

Email: sales@sandstorm.net

Telephone: Call us at (617) 426-5056 between 9AM and 5PM US Eastern Time.

Fax: Fax us at (617) 357-6042.

Web: Use our quote form at http://www.sandstorm.net/products/quote/.